

WHAT IS CLAIMED IS:

1 1. A method of providing a time stamping service for
2 setting a client's system clock, comprising the steps of:

3 a) requesting the time stamping service of a time
4 stamp authority server by a service requester;

5 b) receiving the time stamping service request from
6 said requester and creating and sending a response message
7 corresponding thereto by said time stamp authority server;

8 c) receiving the response message sent from said time
9 stamp authority server and verifying the integrity thereof
10 by said requester;

11 d) downloading a certificate revocation list from a
12 directory server and verifying the validity thereof by
13 said requester; and

14 e) downloading a certificate for an electronic
15 signature of said time stamp authority server from said
16 directory server, verifying an electronic signature value
17 thereof and setting the client's system clock in
18 accordance with the verified result by said requester.

1 2. The method as set forth in claim 1, wherein said
2 step a) includes the steps of:

3 a-1) generating a random number with a given value
4 and setting it as a nonce value of a service request
5 message (TimeStampReq);

6 a-2) setting a requestType parameter of said
7 TimeStampReq message to a getBaseTime value and adding the
8 resulting structure to an extension field of said
9 TimeStampReq message to inform said time stamp authority
10 server that the service request is for the setting of said

11 client's system clock; and

12 a-3) filling other parameters of said TimeStampReq
13 message with given values and sending the resulting
14 TimeStampReq message to said time stamp authority server.

1 3. The method as set forth in claim 1, wherein said
2 step b) includes the steps of:

3 b-1) receiving a service request message
4 (TimeStampReq) sent from said requester and authenticating
5 and verifying the received TimeStampReq message;

6 b-2) if there is an error at said step b-1),
7 processing the received TimeStampReq message as an
8 erroneous message, sending the processed result to said
9 requester and ending the corresponding process;

10 b-3) if there is no error at said step b-1), filling
11 parameters of the response message (TimeStampResp) with
12 given values;

13 b-4) extracting a TSTInfo structure from a
14 TimeStampResp message structure created at said b-3) and,
15 in turn, current time information (a genTime value) from
16 the extracted TSTInfo structure, calculating a message
17 authentication code (MAC) value on the basis of the
18 extracted genTime value and a nonce value, set by said
19 requester and contained in said TimeStampReq message, and
20 setting the calculated MAC value and identifier
21 information of an algorithm used for the calculation of
22 the MAC value respectively in corresponding fields of a
23 MacInfo structure to assure the integrity of said response
24 message;

25 b-5) adding the resulting MacInfo structure to an
26 extension field of said TSTInfo structure and thus

27 completing the creation of said TimeStampResp message
28 structure; and
29 b-6) sending the completed response message
30 (TimeStampResp) to said requester.

1 4. The method as set forth in claim 1, wherein said
2 step c) includes the steps of:

3 c-1) receiving the response message (TimeStampResp)
4 sent from said time stamp authority server and
5 authenticating and verifying the received response
6 message;

7 c-2) extracting a TSTInfo structure from said
8 TimeStampResp message and, in turn, current time
9 information (a genTime value) from the extracted TSTInfo
10 structure, finding a nonce value, set by said requester
11 and sent to said time stamp authority server, and directly
12 calculating a message authentication code (MAC) value on
13 the basis of the extracted genTime value and the found
14 nonce value to check the integrity of said TimeStampResp
15 message;

16 c-3) extracting a MacInfo structure from said
17 TimeStampResp message sent from said time stamp authority
18 server and, in turn, a MAC value from the extracted
19 MacInfo structure and comparing the extracted MAC value
20 with said MAC value calculated at said step c-2) to
21 determine whether the two MAC values are equal; and

22 c-4) if said two MAC values are not equal,
23 recognizing that the current time information (genTime
24 value) sent from said time stamp authority server was
25 altered during the sending and said client's system clock
26 cannot thus be set and then processing the received

27 response message as an erroneous message, and if said two
28 MAC values are equal, recognizing that the integrity of
29 the received response message has been assured.

1 5. The method as set forth in claim 1, wherein said
2 step d) includes the steps of:

3 d-1) downloading said certificate revocation list and
4 said certificate for the electronic signature of said time
5 stamp authority server from said directory server managing
6 certificates of all objects and said certificate
7 revocation list;

8 d-2) extracting time information set to thisUpdate
9 and nextUpdate values from said certificate revocation
10 list downloaded from said directory server, so as to
11 verify the validity of said certificate revocation list on
12 the basis of a genTime value contained in the response
13 message sent from said time stamp authority server; and

14 d-3) determining whether said genTime value is
15 present between said thisUpdate and nextUpdate values, so
16 as to determine whether said certificate revocation list
17 is valid, and if said certificate revocation list is not
18 valid, recognizing that a signature value sent from said
19 time stamp authority server cannot be verified and said
20 client's system clock cannot thus be set and then
21 performing an associated error process.

1 6. The method as set forth in claim 1, wherein said
2 step e) includes the steps of:

3 e-1) extracting desired information from said
4 certificate for the electronic signature of said time
5 stamp authority server and checking whether a serial

6 number of said certificate of said time stamp authority
7 server among the extracted information is present in said
8 certificate revocation list, so as to verify the validity
9 of said certificate;

10 e-2) if the serial number of said certificate of said
11 time stamp authority server is present in said certificate
12 revocation list, recognizing that said client's system
13 clock cannot be set and then performing an associated
14 error process;

15 e-3) extracting a public key from said certificate of
16 said time stamp authority server if the serial number of
17 said certificate is not present in said certificate
18 revocation list;

19 e-4) extracting a signature value from a SignerInfo
20 structure of said TimeStampResp message, decoding the
21 extracted signature value using the extracted public key,
22 extracting a first hash value from the decoded result and
23 directly calculating a second hash value using a digest
24 algorithm of said SignerInfo structure;

25 e-5) comparing said first and second hash values with
26 each other to determine whether they are equal, if said
27 first and second hash values are not equal, recognizing
28 that said time stamp authority server sending said
29 TimeStampResp message is not valid and then performing an
30 associated error process, and if said first and second
31 hash values are equal, recognizing that said time stamp
32 authority server sending said TimeStampResp message is
33 valid; and

34 e-6) setting said client's system clock on the basis
35 of a genTime value extracted from said TimeStampResp
36 message.